Euroopan unionin neuvosto

Bryssel, 10. maaliskuuta 2026
(OR. en)

5134/26

LIMITE

CORLX 10
CFSP/PESC 17
CYBER 4
JAI 21
FIN 8

SÄÄDÖKSET JA MUUT VÄLINEET

Asia:	NEUVOSTON PÄÄTÖS unionia tai sen jäsenvaltioita uhkaavien kyberhyökkäysten vastaisista rajoittavista toimenpiteistä annetun päätöksen (YUTP) 2019/797 muuttamisesta

NEUVOSTON PÄÄTÖS (YUTP) 2026/…,

annettu ... päivänä ...kuuta ...,

unionia tai sen jäsenvaltioita uhkaavien kyberhyökkäysten vastaisista rajoittavista toimenpiteistä annetun päätöksen (YUTP) 2019/797 muuttamisesta

EUROOPAN UNIONIN NEUVOSTO, joka

ottaa huomioon Euroopan unionista tehdyn sopimuksen ja erityisesti sen 29 artiklan,

ottaa huomioon unionin ulkoasioiden ja turvallisuuspolitiikan korkean edustajan ehdotuksen,

sekä katsoo seuraavaa:

(1) Neuvosto hyväksyi 17 päivänä toukokuuta 2019 päätöksen (YUTP) 2019/797[1].

(2) Osana kestäviä, mukautettuja ja koordinoituja unionin toimia jatkuvan kyberuhkan muodostavia toimijoita vastaan kaksi luonnollista henkilöä ja kolme yhteisöä olisi sisällytettävä päätöksen (YUTP) 2019/797 liitteessä olevaan luetteloon luonnollisista henkilöistä, oikeushenkilöistä, yhteisöistä ja elimistä, joihin kohdistetaan rajoittavia toimenpiteitä. Kyseiset henkilöt ja yhteisöt ovat vastuussa vaikutukseltaan merkittävistä kyberhyökkäyksistä, jotka muodostavat ulkoisen uhkan unionille tai sen jäsenvaltioille, tai osallistuvat niihin.

(3) Päätös (YUTP) 2019/797 olisi sen vuoksi muutettava vastaavasti,

ON HYVÄKSYNYT TÄMÄN PÄÄTÖKSEN:

[1] Neuvoston päätös (YUTP) 2019/797, annettu 17 päivänä toukokuuta 2019, unionia tai sen jäsenvaltioita uhkaavien kyberhyökkäysten vastaisista rajoittavista toimenpiteistä (EUVL L 129I, 17.5.2019, s. 13, ELI: http://data.europa.eu/eli/dec/2019/797/oj).

1 artikla

Muutetaan päätöksen (YUTP) 2019/797 liite tämän päätöksen liitteen mukaisesti.

2 artikla

Tämä päätös tulee voimaan päivänä, jona se julkaistaan *Euroopan unionin virallisessa lehdessä*.

Tehty …ssa/ssä … päivänä …kuuta …

Neuvoston puolesta

Puheenjohtaja

LIITE

Muutetaan päätöksen (YUTP) 2019/797 liite seuraavasti:

1) lisätään päätöksen (YUTP) 2019/797 liitteessä olevan otsikon ”A. Luonnolliset henkilöt” alle merkinnät seuraavasti:

	Nimi	Tunnistustiedot	Perusteet	Luetteloon merkitsemisen päivämäärä
”18.	CHEN Cheng	陈诚 (kiinankielinen kirjoitustapa) Peitenimet: Jesse Chen lengmo l3n6m0 Syntymäaika: 20.10.1984 Syntymäpaikka: Yancheng, Jiangsu, Kiina Kansalaisuus: kiinalainen Sukupuoli: mies	Chen Cheng on kiinalainen liike-elämän edustaja, yksi Anxun Information Technology Ltd:n perustajista ja yksi sen pääjohtajista (Chief Operating Officer). Hän on myös kyseisen yrityksen Sichuanin toimipisteen laillinen edustaja. Anxun Information Technology Co. Ltd.-yritys, joka tunnetaan myös nimellä i-Soon, on Kiinan kansantasavaltaan sijoittautunut yritys, joka tarjoaa ”hakkereita vuokralle” (“hacking-for-hire”). Jäsenvaltioiden kriittinen infrastruktuuri ja valtion kriittiset tehtävät ovat olleet Anxun Information Technology Co. Ltd.-yrityksen toimien kohteena. Se on tunkeutunut turvallisuusluokiteltuihin tietoihin ja myynyt niitä. Lisäksi Anxun Information Technology Co. Ltd.-on iskenyt useiden kolmansien valtioiden hallituksia vastaan uhaten näin ollen Euroopan unionista tehdyn sopimuksen 21 artiklan 2 kohdan a–c alakohdassa vahvistettuja unionin yhteisen ulko- ja turvallisuuspolitiikan (YUTP) tavoitteita. Anxun InformationTechnology Co. Ltd saa merkittävää taloudellista hyötyä tarjoamistaan palveluista.	+

+ Virallinen lehti: lisätään tämän päätöksen voimaantulopäivä.

	Nimi	Tunnistustiedot	Perusteet	Luetteloon merkitsemisen päivämäärä
			Sen vuoksi Anxun Information Technology Co. Ltd on vastuussa vaikutukseltaan merkittävistä kyberhyökkäyksistä, jotka muodostavat ulkoisen uhkan unionille ja sen jäsenvaltioille, sekä hyökkäyksistä kolmansia valtioita vastaan. Asemassaan Chen Cheng on vastuussa vaikutukseltaan merkittävistä kyberhyökkäyksistä, jotka aiheuttavat ulkoisen uhkan jäsenvaltioille, sekä vaikutukseltaan merkittävistä kyberhyökkäyksistä kolmansia valtioita vastaan, ja osallistuu niihin.	

	Nimi	Tunnistustiedot	Perusteet	Luetteloon merkitsemisen päivämäärä
19.	WU Haibo	吴海波 (kiinankielinen kirjoitustapa) Peitenimet: shutdown shutd0wn Syntymäpaikka: Kiina Kansalaisuus: kiinalainen Sukupuoli: mies	Wu Haibo on kiinalainen liike-elämän edustaja, yksi Anxun Information Technology Ltd:n perustajista ja yksi sen pääjohtajista (Chief Executive Officer). Hän on myös Anxun Information Technology Co. Ltd:n Shanghain toimipisteen (”mothership”) laillinen edustaja, hallituksen puheenjohtaja ja toimitusjohtaja. Lisäksi hän toimii kyseisen yrityksen Sichuanin toimipisteen laillisena edustajana. Anxun Information Technology Co. Ltd. -yritys, joka tunnetaan myös nimellä i-Soon, on Kiinan kansantasavaltaan sijoittautunut yritys, joka tarjoaa ”hakkereita vuokralle” (“hacking-for-hire”). Jäsenvaltioiden kriittinen infrastruktuuri ja valtion kriittiset tehtävät ovat olleet Anxun Information Technology Co. Ltd. -yrityksen toimien kohteena. Se on tunkeutunut turvallisuusluokiteltuihin tietoihin ja myynyt niitä. Lisäksi yritys on iskenyt useiden kolmansien valtioiden hallituksia vastaan uhaten näin ollen Euroopan unionista tehdyn sopimuksen 21 artiklan 2 kohdan a–c alakohdassa vahvistettuja unionin yhteisen ulko- ja turvallisuuspolitiikan (YUTP) tavoitteita. Anxun Information Technology Co. Ltd. saa merkittävää taloudellista hyötyä tarjoamistaan palveluista.	[+]”;

[+] Virallinen lehti: lisätään tämän päätöksen voimaantulopäivä.

	Nimi	Tunnistustiedot	Perusteet	Luetteloon merkitsemisen päivämäärä
			Sen vuoksi Anxun Information Technology Co. Ltd. on vastuussa vaikutukseltaan merkittävistä kyberhyökkäyksistä, jotka muodostavat ulkoisen uhkan jäsenvaltioille sekä hyökkäyksistä kolmansia valtioita vastaan. Wu Haibo osallistui jäsenvaltioihin kohdistettujen vaikutukseltaan merkittävien kyberhyökkäysyritysten johtamiseen ja edistämiseen. Tässä ominaisuudessa hän on vastuussa vaikutukseltaan merkittävistä kyberhyökkäyksistä, jotka aiheuttavat ulkoisen uhkan jäsenvaltioille, sekä vaikutukseltaan merkittävistä kyberhyökkäyksistä kolmansia valtioita vastaan, ja osallistuu niihin.	

2) lisätään päätöksen (YUTP) 2019/797 liitteessä olevan otsikon ”B. Oikeushenkilöt, yhteisöt ja elimet” alle merkinnät seuraavasti:

	Nimi	Tunnistustiedot	Perusteet	Luetteloon merkitsemisen päivämäärä
”5.	Integrity Technology Group	永信至诚科技集团股份有限公司 (kiinankielinen kirjoitustapa) Alias: Beijing Integrity Technology Company Limited, Yongxin Zhicheng Technology Group Company Limited Osoite: Fenghao East Road, Room 103, Building 6, No. 9, Haidian District, Peking, Kiina	Integrity Technology Group on Kiinan kansantasavaltaan sijoittautunut kyberturvallisuusyritys, joka mahdollisti edistyneeseen pitkäkestoiseen uhkaan (APT) Flax Typhooniin yhdistettyjä kyberhyökkäyksiä. Kyseinen APT hyödynsi Integrity Technology Groupin tuotteita ja teknologiaa tietokoneverkkojen hyväksikäyttöön liittyvässä toiminnassaan. Integrity Technology Groupin tuotteita on sen jälkeen käytetty esineiden internetin laitteiden vaarantamiseen ja niihin tunkeutumiseen jäsenvaltioissa, maissa muualla Euroopassa ja ympäri maailmaa. Vuosina 2022–2023 Flax Typhoon tunkeutui vähintään 65 600 esineiden internetiin yhdistettyyn laitteeseen kuudessa jäsenvaltiossa Integrity Technology Groupin tuotteiden avulla. Näin ollen Integrity Technology Groupin kaupallisia tuotteita ja infrastruktuuria käytettiin rutiininomaisesti jäsenvaltioihin ja kolmansiin valtioihin kohdistetuissa kyberhyökkäyksissä. Koska Integrity Technology Group vaikuttaa digitaaliseen infrastruktuuriin liittyviin tietojärjestelmiin, se tarjoaa näin ollen teknistä ja aineellista tukea vaikutukseltaan merkittäville kyberhyökkäyksille, jotka muodostavat ulkoisen uhkan jäsenvaltioille ja kolmansille valtioille.	+

+ Virallinen lehti: lisätään tämän päätöksen voimaantulopäivä.

	Nimi	Tunnistustiedot	Perusteet	Luetteloon merkitsemisen päivämäärä
		Rekisteröintipaikka: Peking, Kiina Rekisteröintipäivä: 2.9.2010 Rekisteritunnus (Unified Social Credit Code): 91110108562135265P		

	Nimi	Tunnistustiedot	Perusteet	Luetteloon merkitsemisen päivämäärä
6.	Emennet Pasargad	Alias: Anzu Team, Holy Souls, Aria Sepehr Ayandehsazan, Haywire Kitten Rekisteröintipaikka: Teheran, Iran Rekisterinumero: 554267 Päätoimipaikka: Teheran, Iran	Emennet Pasargad on iranilainen kybertoimija (yritys), joka on kohdistanut iskuja useisiin yhteisöihin erityisesti jäsenvaltioissa ja Yhdysvalloissa. Anzu Team -nimellä toiminut Emennet Pasargard kohdisti toimia Ruotsin digitaaliseen infrastruktuuriin ja vaaransi ruotsalaisen tekstiviestipalvelun toiminnan, mikä vaikutti suureen määrään ihmisiä. Holy Souls -nimellä toiminut sama yhteisö vaaransi ranskalaisen satiirisen Charlie Hebdo -lehden tilaajatietokannan ja ilmoitti sen myytäväksi pimeässä verkossa. Emennet Pasargad vaaransi mainostaulujen toiminnan Pariisin olympialaisten aikana ja sai ne esittämään disinformaatiokampanjoita. Emennet Pasargad yritti myös sekaantua Yhdysvaltojen vuoden 2020 presidentinvaaleihin uhaten demokratiaa ja oikeusvaltiota hankkimalla luottamuksellisia tietoja yhdysvaltalaisista äänestäjistä ja tunkeutumalla luvattomasti yhdysvaltalaisen mediayhtiön tietokoneverkkoon. Sen vuoksi Emennet Pasargad on vastuussa vaikutukseltaan merkittävistä kyberhyökkäyksistä, jotka aiheuttavat ulkoisen uhkan jäsenvaltioille, sekä vaikutukseltaan merkittävistä kyberhyökkäyksistä kolmatta valtiota vastaan.	[+]

[+] Virallinen lehti: lisätään tämän päätöksen voimaantulopäivä.

	Nimi	Tunnistustiedot	Perusteet	Luetteloon merkitsemisen päivämäärä
7.	Anxun Information Technology Co. Ltd.	安洵信息技术有限公司 (kiinankielinen kirjoitustapa) Alias: i-Soon Osoite: Room 1002, Qiangqiang Building, No. 1318 Qixin Road, Minhang District, Shanghai Rekisteritunnus (Unified Social Credit Code): 91510105332025597A (Sichuanin toimipiste) Rekisteritunnus (Unified Social Credit Code): 91310116561906136G (Shanghain toimipiste)	Anxun Information Technology Co. Ltd. on Kiinan kansantasavaltaan sijoittautunut yritys, joka tarjoaa ”hakkereita vuokralle” (“hacking-for-hire”). Jäsenvaltioiden kriittinen infrastruktuuri ja valtion kriittiset tehtävät ovat olleet sen toimien kohteena. Se on tunkeutunut turvallisuusluokiteltuihin tietoihin ja myynyt niitä. Lisäksi Anxun Information Technology Co. Ltd. on iskenyt useiden kolmansien valtioiden hallituksia vastaan uhaten näin ollen Euroopan unionista tehdyn sopimuksen 21 artiklan 2 kohdan a – c alakohdassa vahvistettuja unionin yhteisen ulko- ja turvallisuuspolitiikan (YUTP) tavoitteita. Anxun International Technology Co. Ltd. saa merkittävää taloudellista hyötyä tarjoamistaan palveluista. Sen vuoksi Anxun Information Technology Co. Ltd. on vastuussa vaikutukseltaan merkittävistä kyberhyökkäyksistä, jotka muodostavat ulkoisen uhkan jäsenvaltioille, sekä vaikutukseltaan merkittävistä kyberhyökkäyksistä kolmansia valtioita vastaan.	[+]”.

[+] Virallinen lehti: lisätään tämän päätöksen voimaantulopäivä.

	Nimi	Tunnistustiedot	Perusteet	Luetteloon merkitsemisen päivämäärä
		Verkkosivusto: i-soon.net, isoon.net, i-soon.com.cn, isoonren.com, isoon.win Puhelinnumerot: +862161119992, +8605645893417, +8613761671735, +864000665915 Sähköposti: shutdown@163.com, isoon2015@126.com, tao_tingting@i-soon.net, li_ping@i-soon.net		